MUANGTHAI CAPITAL PUBLIC COMPANY LIMITED

332/1 Jaransanitwong Road, Bangplad, Bangplad, Bangkok Thailand 10700 Tel. +662 483 8888

Information Security Policy

1. Objectives

Muangthai capital Public Company Limited and its subsidiaries ("the Company") aims to provide appropriate shared services in line with business policies and prevent problems that may arise from improper use of information technology network systems by users and various threats. The Company has created this information system security policy and measures as a guideline for determining procedures for inspecting and maintaining the security of information systems to ensure continuous security and service. Moreover, it is to reduce information technology risks and cyber threats to maximize user confidence.

The Company has established policies and measures to maintain information system security for executives, employees of the Company, and third parties related to the Company to use as guidelines for operating in accordance with the law and the official regulations mentioned above by repealing the Information Security Policy dated May 9, 2014.

2. Duties and responsibilities according to policy

2.1 The Board of Directors is responsible for approving policies and measures for maintaining information security and giving importance to preventing problems from using the information technology network in an incorrect manner by users and threats. It also covers the assignment of information risk assessments under appropriate risk management supervision.

2.2 Top executives are responsible for supervising operations to be in compliance with the law and other related official regulations.

2.3 Employees must comply with this policy, regulations, orders and manuals regarding information system security measures.

3. Definitions

"the Company" means Muangthai capital Public Company Limited and its subsidiaries.

"Information Technology Department" means the department responsible for managing the Company's information technology.

"Employee" means employees hired as interns, probationary employees, regular employees, special contract employees and executives at all levels under the employment of the Company.

"User" means employees of the Company and third parties who are authorized to have passwords to use the Company's information technology.

"Privileged user" means users who have higher privileges than system administrators and general users who are assigned to make changes or modifications to systems and databases.

"Information System Administrator" means the internal information department that possesses the computer system and has responsibility for the computer system.

"Administrator" means a person assigned to manage, operate, and maintain computer and information systems.

"Third Party" means a person or legal entity that the Company or its divisions allow to have access to data or information systems according to the type of use and is responsible for not disclosing the Company's secrets without permission.

"Department Manager" means the person responsible for internal departments according to the Company's corporate structure.

"Computer system" means all types of computer tools or equipment, whether hardware and software of all sizes, network equipment, both wired and wireless, materials and equipment for storing and transferring various types of data, Internet systems, and Intranet systems, including various electrical and telecommunications equipment that can work or be used in the same or similar manner to a computer, both being the property of the Company, partner companies and other companies that are in the process of installation and have not yet been delivered, or of employees who install or use within the Company's establishments

"Information" means information, news, records, history, text in documents, computer programs, computer data, images, sounds, signs, and symbols, regardless of whether it is in a form that can convey meaning to a person to understand directly or through any tool or device.

"Information Assets" means hardware assets such as computers and various computer equipment, communication devices, and information assets whether in electronic or document form such as databases, data files in actual systems, backup data, system user manuals, system development documentation, various contracts, etc.

" Data Owner" means the Company or person assigned to maintain data in accordance with this policy.

4. The Information Security Policy consists of the following sections:

<u>Section 1</u> Access control and user authentication

The Company has clearly defined the roles and responsibilities of each department, as well as controls access to information systems, user authentication, and prevention of disclaimers in accordance with the following policies:

1. Determination of personnel or information system units and appropriate division of authority and duties in information system management.

All employees are responsible for maintaining information security and adhering to information security policies and procedures. It includes a clear division of duties between each department in order to balance all operations.

1) In cases where any employee's duties involve sensitive or confidential information, it is necessary to define information security duties and responsibilities that are specific to that job in the job description.
2) The human resources department must create awareness of information security responsibilities from the time of hiring employees, including specifying such responsibilities in the employment contract.
3) Conditions of employment should specify information security responsibilities and compliance with information security policies. Violating or neglecting the duties and information security policy of the Company is considered an offense. The Company's penalties must be considered, which depends on the severity of the impact.
4) Agencies or individuals from outside agencies hired by the Company must understand and be informed of the essential information security policy, especially the non-disclosure of information, before actually performing any work in the Company.
5) Employees are responsible for maintaining the confidentiality of information when working outside of the office building, at home, or logging into an external Company system (Remote Access).
6) Users, employees, and external agencies must comply with the Company's information security policies and procedures. All employees should receive periodic additional information security awareness training to stay informed of the Company's additional security policies including security breach incidents and new case studies to highlight the Company's information security policies.
7) The human resources and legal departments must determine penalties for employees violating the information security policy and related procedures.

2. Access Control in Information Technology System

All Company departments involved with data and information systems must maintain an inventory of the Company's information assets.

1) The person responsible for information assets must regularly review and update the information assets account and notify of any changes at least once a year.
2) Each agency must designate an information asset owner who is responsible for maintaining that information asset. In the case of information assets that may have multiple owners, senior management must assign responsibility to those who use or are most involved with that specific information.

3) The asset inventory is confidential information that is allowed to be disclosed or accessed only by relevant and necessary persons.
4) Users, employees, and third parties must agree to abide by the terms of use of data and information assets.
5) Permission to access confidential information must be made by the owner of the information in determining the right to access the information based on business necessity.
6) Employees must be aware of their duties and responsibilities in disclosing and sharing information both within the Company and outside agencies.
7) The Human Resources Department must notify the Information Technology Department and related departments immediately upon transfer, resignation or termination of employment of the Company in order to withdraw rights to use various work systems and enter and exit the Company area. In addition, the Company's assets must be returned to the person responsible for those assets.
8) It is necessary to define security control areas within the Company and appropriate preventative measures according to the level of risk in each area. It is to protect a Company's basic information and information processing systems from unauthorized access, potential damage from threats and interference, whether intentional or natural disasters.
9) It is necessary to prioritize the areas in the Company's office and determine control areas through risk assessment. It is to define the security control area and organize appropriate control measures for that area.
10) Employees must attach their employee ID card during business hours while at the Company's office building. Such rights must be terminated immediately upon resignation or termination of employment.
11) The contact person must contact the security guard to exchange the card for permission to enter the premises and the card must be displayed at all times while in the Company office building.
12) Building with computer center Computer or communication system rooms must have strict security measures. To prevent the entry and exit of unauthorized persons.
13) The area where the entry-exit control equipment is installed must prohibit employees from avoiding or refraining from operating such equipment, such as opening it from the inside and allowing people from the outside to enter without controlling, following or contacting.
14) The processing room in the computer center is a restricted area. Programmers and general users do not have the right to enter such areas without control. Additionally, there should be no signs or symbols indicating the location of the computer center.
15) Backup devices and media must be stored in a secure location away from the primary storage device to prevent damage in the event of an emergency in the primary storage area.

16) Computer centers must have safety controls that may result from floods, earthquakes, or fires. There must also be an air conditioning and humidity system, an electrical current system, and a lightning protection system installed in every building. Equipment must be arranged to minimize unnecessary access to the work area to avoid unauthorized access. It also covers placing the device at an appropriate angle to reduce the risk of data being viewed by unrelated and unauthorized persons during use. Such equipment requires controlled environmental conditions such as temperature and humidity, which can cause malfunctions of information processing equipment. Important computer and network equipment must have an Uninterruptible Power Supply (UPS) and Power Generator to facilitate continuous operation of the system or to stop working properly when the power system is interrupted. It also requires regular inspection of the Uninterruptible Power Supply (UPS) according to the manufacturer's procedures.

3. Identity verification and protection for disclaimers

To reduce risk and prevent unauthorized access, it is necessary to control access to information systems based on business needs and requirements as well as security requirements. There needs to be a way to control rights in the process involving users of the system, from requesting registration to canceling rights if the user is no longer needed including controlling privileged users who can modify various rights of the system.

1) Every user must have a unique user ID to identify and track each user's activity.
2) Every employee who has access to the information system must have a unique user ID to enter the system. The password must belong to the requester only.
3) Users of the Company's system must sign to acknowledge the rules and conditions for using the Company's system and agree to abide by the rules for using the system.
4) All privileged users must have a personal password for normal operations according to their responsibilities and job needs only. However, the Information System Administrator will be the one to consider granting or withdrawing such rights.
5) Information administrators must determine the frequency of reviewing user access rights and immediately revoke access of users who do not have such rights from the system to prevent unauthorized use and access.
6) Users are obliged to set and use a password that is secure and difficult to guess, confidential and not share or disclose it to any other person. Users must change their passwords regularly.
7) Users must change the temporary password received immediately upon first login to prevent hacking.
8) Users should log out of the network immediately when finished or not needed. If not used for a long time, the user should turn off the computer or terminal. However, if it is found that the system has not been used within the specified time, the system must automatically disconnect from the system.

9) The use of a shared username or "GUEST" is only permitted for business or important technical reasons. It requires additional controls to be able to identify and track individual user usage.

10) The Company has established multi-factor authentication for all Privileged User accounts of operating systems, database systems, work systems, network devices, and network security devices. It covers all user accounts that can access customer data across operating systems, databases, applications, network devices and network security devices connected to an internet-facing network.

<u>Section 2</u> Maintaining the confidentiality and the integrity of the information system

The Company has established measures to maintain the confidentiality of information and the integrity of the information system according to the following policies:

1. Confidentiality

The Company has established appropriate procedures, and methods for data transmission, processing, storage, and destruction to maintain the confidentiality, and integrity of the data.

1) The Company must consider the hierarchy of data and guidelines for managing data within that hierarchy. It is important to consider the following encryption hierarchy:

1.1) Level 1: General information (can be disclosed)

Information that is generally available to third parties without being blocked or affecting operations. It can be presented to the public and is not of direct commercial benefit to competitors or information that is legally required to be disclosed. However, documents must be disposed of by shredding or burning and electronic media must be disposed of by erasing data.

1.2) Level 2: Internal use information

It is information that the data owner considers that it can be disclosed to all employees within the Company but cannot be disclosed to people outside the Company as it may cause damage to the Company. If there is a request from a third party, the data owner must exercise discretion in disclosing it based on necessity for use. However, documents must be disposed of by shredding or burning and electronic media must be disposed of by erasing data or appropriate measures.

1.3) Level 3: Confidential Information

It is information for internal use within the Company where the owner of the information considers that it cannot be disclosed to all employees. This type of information will only be given to those involved and required to do their job. It must be used according to the rights and necessities that should be known to be sufficient for the operation. However, documents must be disposed of by shredding or burning and electronic media must be disposed of by erasing data, overwriting data, program instructions, magnetic fields, or smashing.

2) Data owners are responsible for defining the data hierarchy with business needs and impacts in mind.

3) Because the data hierarchy may change over time, data owners must regularly review the data hierarchy to reflect the current state of the data.

4) Sensitive data must have a responsible custodian and must protect the data according to practices consistent with the data hierarchy.

5) Changes to the data protection level and data hierarchy require the agreement and approval of the data owner. For the transmission, processing and storage of confidential data securely and sensitively to prevent alteration by unauthorized or unauthorized persons, the Company has arranged for the transmission of data through the Intranet network system, including data processing by secure servers and standard data storage locations according to this policy.

2. System development, change control, improvement of information systems or information processing equipment.

The Company has established operational policies and internal controls for the development, control of change, and improvement of information systems to reduce abnormal operation or risk of damage to the information system.

2.1 Confidentiality

1) Information system administrators must determine information security needs before developing or acquiring systems. It must be in writing and follow Company policies and standards in developing work systems.

2) The processing system must be designed to be able to be reviewed in order to detect any errors or damage in data processing, including reporting errors from processing such as system failure messages, etc.

3) It is necessary to check the accuracy of the resulting data from the computer system to ensure the integrity of the data.

4) There must be regulations in place in case errors in the resulting data are discovered, including determining the responsibilities of those involved.

5) It is necessary to establish regulations regarding the use of encryption, including software and encryption standards that allow use of data in different hierarchies. Additionally, it is necessary to keep the list of software and encryption standards up to date.

6) Before a new version is released into production, it is necessary to obtain approval documents for use of the new version and other supporting evidence such as test reports to verify authenticity from users. It must modify the source code in the library accordingly by having a backup and storage of the pre-modified version of the program to be reused when necessary, such as the date, month, and year of use.

7) It must not store the source code of the program on the production system. It requires keeping records for auditing various modifications to source code and programs.

8) In cases where copies of data from a production system are used to test newly developed systems, it is necessary to control the test data in the same way as the data in the production system. Permission must be obtained before a physical copy of the data is used in a test environment each time. There is control over access to data in system testing and the test data is deleted from the system immediately upon completion of testing. It is necessary to store an Audit Log to monitor testing activities.
9) It requires the appointment of a library administrator to store the source code and to limit access to the program's source code.

2.2 System development, change control, improvement of information systems or information processing equipment

The Company has set minimum security standards and set up the security of systems and information processing equipment to be consistent with the provision of services. It is based on the ISO-IEC 27001:2013 Information Security Management Systems standard, including measures and regulations according to relevant laws to ensure the security of information systems. In addition, the Company has organized regular system development and review.

1) Improving the system or program must be in accordance with regulations regarding the improvement and modification of work systems or programs. It is necessary to have a written and trackable status such as a test plan for system program modifications and test results.
2) Each system administrator must make a written request for approval to modify the system or program from the information system administrator, specifying the computers, software, and databases that must be changed. It includes protection against potential operational impacts, backing up data before updating or maintaining the system, keeping documentation of changes up to date, controlling version changes and keeping records to verify corrections.

2.3 Using information technology services from external service providers

1) It requires a written contract specifying the scope of operations, duties and responsibilities of the contracting parties.
2) It requires risk management in using services from external service providers by considering appropriate selection, monitoring, evaluation and inspection of services.
3) It requires a written contract to maintain data security, including confidentiality and related laws.
4) It requires a contingency plan from an external service provider for information technology operations in accordance with the Company's information technology contingency plan.

2.4 Service network management

The Company has established measures to prevent unauthorized access to the network service system as follows:

1) Information administrators are responsible for setting measures to control network connections and allowing connections by external devices.
2) Registration is required to verify your identity in order to use the network through the Company's security system.
3) There must be a clear separation of network types according to the type of information service group and the level of importance of the data.
4) The Company prohibits the use of software or data from outside parties unless permitted by the Information System Administrator and must inspect such software or data to ensure that there are no computer viruses or hidden dangerous software.
5) The Company provides anti-virus and anti-malware programs to be installed and updated at all times at the operating system level on computers and servers to reduce the risk of viruses and malware.

Section 3 Maintaining the availability of services

The Company has established measures to provide efficient service and availability of services at all times to support transactions according to business needs continuously, including proper data backup to recover the system from damage according to the following policies:

1. Assessing risk management of service systems

The Company provides risk assessment and management by establishing concrete risk assessment methods, analyzing and evaluating the impact on the business that may result from security failures. It also includes setting risk tolerance criteria and acceptable risk levels, along with identifying and evaluating risk management options and possible actions to avoid risk and reduce damage. The Company will regularly review risks.

2. Tracking and investigating irregularities and vulnerabilities of information systems

The Company arranges for the monitoring of unusual cases and the possibility of threats as well as illegal access to information systems. The Security Patch management process for all work systems and devices can assess system vulnerabilities, prepare solutions, or close vulnerabilities from system vulnerabilities, especially network systems related to service provision including work system programs and databases in cases where the system is at high risk, such as a system that provides services over a public network should have a Penetration Test for the effectiveness of security technology. The Company will install equipment and develop software systems to comply with the policy.

3. Troubleshooting, recording events, and reporting information system damage

The Company has established procedures for solving problems, teams or responsible persons, including methods for reporting problems to executives and informing relevant people in order to collect various useful evidence. It also covers recording incidents or producing written reports as a solution.

4. Backing up data

The Company provides backups of important data and other information necessary for operations so that information is readily available within the country for conducting business and providing continuous service to customers. It also covers determining appropriate backup practices or procedures. It must be consistent with the risks of the format or nature of providing important payment system services, supervised payment system business and supervised payment services, as the case may be. Such as data to be backed up, frequency of backup, media used, storage location, storage method and use. It is necessary to regularly test the backup data at least once a year and in accordance with the Company's backup policy.

5. Preparing business continuation plans or emergency plans for information systems

The Company provides analysis and identification of risks and important operations of the service. It also covers Recovery Time Objectives and provides a written plan with detailed steps to take when there is a major operational disruption to be able to operate within the specified period according to the details and requirements specified in the information system security policy and measures. Additionally, training, testing, and review of plans for the implementation of important tasks are organized at least once a year or when factors affecting risk are changed.

Section 4 Information system security audit

To ensure that the policies and measures for maintaining information system security related to the provision of services are efficient, stable and safe and can provide services continuously, the Company arranges regular inspections of information system security at least once a year. It also covers the preparation of audit results reports to the Board of Directors or assigned committees and notify relevant internal departments for implementation as well as sending a copy of the inspection results to the Bank of Thailand within 45 days from the date the inspection is completed. It also includes monitoring and inspecting the provision of supervised payment systems and submitting reports to ensure compliance with all relevant regulations to avoid violating legal requirements.

Section 5 Reviewing or Improving Information System Security Measures

The Company or the designated person must review this policy regularly at least once a year and must submit it to the board of directors for approval if there are any changes.

This policy has been considered and approved by the Board of Directors. It has been effective from 9 May 2023 onwards.

Adm. Apichart Pengsritong
Chairman of the Board of Directors